The way Hacker uses to remain anonymous

Hackers use different ways to remain anonymous while hacking, but it must be said that anonymity is completely unthinkable, but hackers can be safe and anonymous to some degree and ensure backwardness. It is very difficult.

Hackers use different ways to remain anonymous while hacking, but it must be said that anonymity is completely unthinkable, but hackers can be safe and anonymous to some degree and ensure backwardness. It is very difficult. Here are some methods to help anonymous hackers while entering a system.

1. Do not use Windows

Windows is full of vulnerabilities that can be exploited. Every month, Microsoft releases security patches with the latest fixes. These vulnerabilities can allow spyware to penetrate, completely overcome all your anonymity efforts. Any hacker who wants to remain anonymous will avoid Windows as a plague. Instead, they use secure open source open source operating systems, such as Tails and Whonix.

1. Interesting operating systems may be unknown to you

2. Do not connect directly to the Internet

Avoid people tracking your real IP address through the use of VPN and TOR services.

VPN allows users to create a private tunnel. Anyone trying to track from the Internet can only view the VPN server's address, which can be a server located in any country in the world you choose.

1. 11 best VPN software

2. How to secure your VPN more secure?

TOR is a network of entire routing nodes for your traffic. Each node in the transmission line only knows the IP of the previous node. Finally, the traffic passes through the regular Internet from one of these nodes, called exit points. The most perfect approach is to combine both and use the VPN before entering the TOR.

1. Using Tor, I2P or safer VPN?

In addition, hackers use proxy chains, which allow hackers to route their traffic through a variety of anonymous and proxy servers by hiding behind them. In fact, it makes proxy servers forward requests from hackers so that the request appears to be from a proxy server not from hacker servers. Hackers really cause traffic to pass through proxies and therefore their IP is changed many times and the original IP is not displayed.

1. What is the difference between Proxy and VPN?

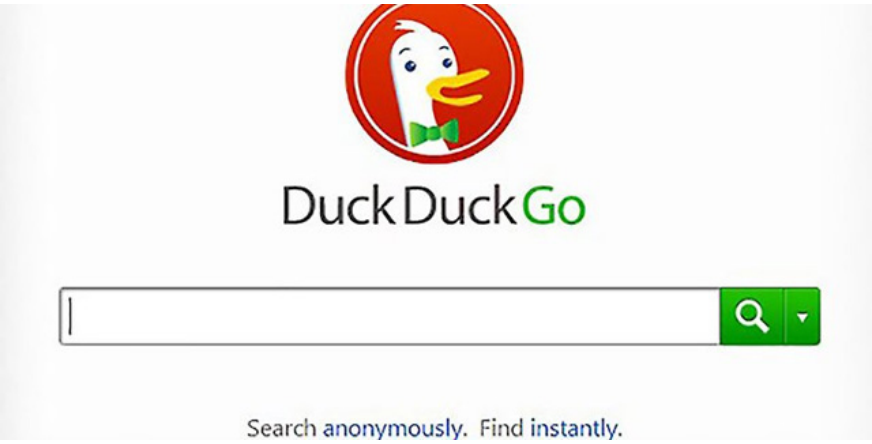
3. Do not use real email addresses

Instead, use anonymous or remailer email services. Anonymous email services allow you to email someone without leaving any trace, especially if combined with VPN or TOR access. Remailer is a service where you can use your real email account to send email and it will forward that message in anonymous mode. Some remailers can also resend the mail, but this could be the 'sticking his back' action. It can record your real address, but the remailer can add additional anonymous layers to ensure security.

1. 8 best secure email services ensure your privacy

4. Do not use Google

Google tracks everything you do to serve their ads that users can click on. There are many ways to exploit this useful search engine without leaving an identity like the StartPage service for google results without storing IP addresses, cookies or search results. DuckDuckGo is the same service.



In addition, Tor Browser is also a smart choice. When using this browser, traffic or computer-derived packets are made to go through a certain point called node. During the process of requesting a specific website, the IP address will be changed many times and cannot determine your IP address because the browser has created encryption classes. Therefore hackers can browse the Internet anonymously. In addition, Tor browser also allows you to access Dark Web or hidden web.

1. A guide to the Deep Web for newbies

5. Do not use public Wifi

There are two problems here, one is that the unique MAC address will be reruned by the router in public, although you can avoid this by using MAC spoofing. If you ever get back to the real MAC address, you can find the original computer, plus the shop's CCTV can record the image and your identity will be retrieved. Secondly, Wifi attack is very popular, man-in-the-middle attack technique via Wifi will reveal all your anonymity efforts. However, other hackers will need to be on the same physical Wi-Fi network to know your identity.

1. Using public wifi is easy to be attacked by hackers
2. How easy is Crack WiFi?

6. Use Macchanger

MAC stands for Media Access Control. Changing the Mac is one of the hackers' needs to remain anonymous. Each device has a unique MAC address provided by the respective manufacturer. The transferred packets have a source MAC address and destination MAC address. Now, if the packet is blocked or monitored, the MAC address can be identified and easily traced to the hacker. Therefore, hackers often change their MAC address before performing attacks.

1. 2 simple ways to view and read MAC addresses on Windows 10 computers

Real hackers can add multiple layers of security to anonymize their activities. However, the above six ways are the most useful ways.

See more:

1. The most basic insights to becoming a Hacker - Part 1

2. In addition to white hat hackers and black hat hackers, what other colors are available to hackers? Is there any genuine work for them?
3. How Hacker works

You finished reading the article "**The way Hacker uses to remain anonymous**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
